Additionally, Sony describes the use of random numbers in it's authentication method, and as stated by the Examiner on page 4 of the Office Action, Sony does not describe the use of signatures, whereas Spies describes computing the hash of a document, and does not describe the use of random numbers.

In particular, the document described in Spies, cannot be analogous to a random number as Spies describes "the originating participant 22(a) constructs the appropriate commerce document and commerce instrument for the commercial transaction" (column 12 lines 1 to 3).

Hence, the document is selected by the originating participant, and is not random. Thus, the proposed modification of Spies renders Spies unsatisfactory for its intended purpose, and changes the principle operation of Spies, which means that, in accordance with MPEP 2143, Spies cannot be combined with Sony.

Accordingly, there would be no motivation for persons skilled in the art to combine the teachings of Sony and Spies, as the prior art references teach away from each other.

However as the Examiner believes that the references can be combined, the applicant now addresses the combination.

The present claim 1 requires:

1. generating a secret random number;

2. calculating a signature for the random number using a signature function, in a trusted authentication chip;

3. encrypting the random number <u>and</u> the signature by a symmetric encryption function using a first key, in the trusted authentication chip;

4. passing the encrypted random number and the signature from the trusted authentication chip to an untrusted authentication chip;

Sony describes a reader/writer transmitting C1 (code) to an IC card such that a random number RA is encrypted using a key KB (see abstract). As the Examiner has stated on page 4 of the Office Action, Sony does not describe the calculating a signature for the random number.

With respect to Spies, Spies describes generating the hash of a document, and encrypting the hash of the document with an asymmetric key. The hash is then added to the document, where the combined hash and document are encrypted with another (symmetric) key, before sending the document from the originating computing unit 24(a) to a recipient (see column 12 lines 6 to 25).

Thus, a combination of Sony and Spies would describe generating a random number and encrypting the random number with a key, computing the hash of a document (and instrument) through the use of a hashing algorithm, encrypting the hash using an asymmetric key, encrypting the document and added hash with a symmetric key, then forwarding the encrypted random number, and encrypted hash function and document, where the random number and the encrypted hash function and document are encrypted with two different keys.

Therefore, a combination of Sony and Spies would not teach the random number and the signature being enciphered by the same key. This is in no way taught or described by either Sony, Spies, or a combination thereof.

Additionally, claim 1 further describes that once the encrypted random number and signature have been transmitted:

1. decrypting the encrypted random number and signature with a symmetric decryption function using the first key, in the untrusted authentication chip;

2. comparing the signature calculated in the untrusted authentication chip with the signature decrypted; and,

3. in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

In contrast, Sony describes that once the reader/writer transmits to the IC card a code C4 (including plain text M3 encrypted using key KB):

1. IC card decrypts code C4 into plain text M4 using key KB.

2. When IC card determines plain text M4 and random number RB are the same, the R/W is authenticated.

Spies describes that once the recipient has verified the received data, "the participants can return the appropriate receipts" (see column 14 lines 35 to 45). Thus, the combination of Sony and Spies would not describe that in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using a second key and returning it to the trusted authentication chip.

Furthermore, claim 1 further describes, that once the encrypted random number is returned to the trusted authentication chip:

1. encrypting the random number by the symmetric encryption function using the second key, in the trusted authentication chip;

2. comparing the two random numbers encrypted using the second key, in the trusted authentication chip;

3. in the event that the two random numbers encrypted using the second key match, considering the untrusted chip to be valid, and otherwise, the chip is invalid;

which, neither Sony, Spies, or a combination thereof describe.

Therefore, the combination of Sony and Spies does not describe the use of a first key to encrypt a random number and a signature by a symmetric encryption function, comparing two signatures in an untrusted chip, and in the event that the two signatures match, encrypting the decrypted random number by the symmetric encryption function using the second key and returning it to the trusted authentication chip, and further still, once the data is returned to the trusted authentication chip, encrypting the random number by the symmetric function using the second key, and then comparing the two random numbers.

The Applicant respectfully reminds the Examiner that MPEP 2143 requires that the prior art reference (or references when combined) must teach or suggest all the claim limitations. As there are numerous features of claim 1 that are not taught by Sony, Spies, or a combination of thereof, the case for *prima facie* obviousness has not been established.

Additionally, the Applicant respectfully submits, that as claim 1 recites a different security system to the combination of Sony and Spies, it will be appreciated by the Examiner, that these differences in security systems are not trivial, and present numerous advantages, including increasing the efficiency of authenticating an untrusted chip.

Therefore, in view of the above comments, claim 1 is patentable over Sony in view of Spies.

In light of the above, it is respectfully submitted that the claim rejections have been successfully traversed and addressed. Accordingly, it is respectfully submitted that the claims, and the application as a whole with these claims, are allowable, and a favourable reconsideration is therefore earnestly solicited.

Very respectfully,

Applicants:

SIMON ROBERT WALMSLEY

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia
Email: kia.silverbrook@silverbrookresearch.com
Telephone: +612 9818 6633
Facsimile: +61 2 9555 7762